Why Cyber Security and Chemical Security Go Hand in Hand

by Emily Zurawski, August 2, 2016

Many of us protect our laptops and cellphones from being hacked, so why aren't we protecting our communities from chemical plants that are subject to hacking?

President Barack Obama delivers remarks during a memorial service at Baylor University in Waco, Texas, for victims killed last week at a fertilizer plant explosion in West, Texas, April 25, 2013. (Official White House Photo by Pete Souza)

> "The collective result of these kinds of attacks could be a cyber Pearl Harbor … In fact, it would paralyze and shock the nation and create a new, profound sense of vulnerability." *Former Secretary of Defense Leon Panetta, October 11, 2012*

In late April 2016, the Russian government reportedly hacked the Democratic National Committee. In a recent 60 minutes report, the susceptibility of cell phones was highlighted. Both of these instances show how vulnerable almost everything is on the internet. There's a common saying in the cyber security field, "There are two types of institutions, those that have been hacked and those who don't know they've been hacked." Most of us try to protect ourselves and our businesses from hacking, but according to the annual Verizon report, the majority of businesses have already been hacked. Now, the Democratic National Committee is among them.

But cyber vulnerability isn't just a business concern — it could actually threaten the lives and safety of more than 100 million Americans. Secretary Panetta goes on to describe that, "We know that foreign cyber actors are probing America's critical infrastructure networks. They are targeting the computer control systems that operate chemical, electricity and water plants and those that guide transportation throughout this country."

In fact, in November 2011, it was also reported that Russian hackers gained control of a water treatment plant in Illinois. The hackers allegedly broke various pumps by commanding the pumps to turn on and off quickly. Later that month, another hacker named "pr0f" infiltrated the network of a water treatment plant in South Houston, Texas. He did so simply to show the vulnerability of these systems to hackers.

The vulnerability of these plants to cyber or physical attacks, accidents or natural disasters puts millions of Americans at risk on a daily basis. A single release of a poison gas, such as chlorine, can endanger the lives of thousands of people. No requirements are currently in place to eliminate this hazard at the highest risk facilities; only a switch to safer available chemicals or processes can truly eliminate these catastrophic hazards.

Addressing these hazards quickly is a must. Right now, **466 chemical facilities each put 100,000 or more people at risk if there were to be a chemical release.** One out of every ten children in the United States lives and goes to school within one mile of a dangerous chemical facility. This means 4.6 million schoolchildren are in danger every single day in the United States.

We have known for how to prevent these disasters since before 9/11, but have done nothing to require it. Chemical plants can switch to less harmful, less toxic materials often for minimal cost, maximizing community benefits and rendering cyber or physically attacks and other disasters irrelevant.

After 9/11, noting magnitude of the hazard, Washington DC switched its main waste water treatment plant to virtually harmless sodium hypochlorite bleach within 90 days. Moreover, all U.S. Clorox facilities eliminated their hazard by switching from chlorine to the same high strength bleach. In the past 15 years, hundreds of other chemical facilities have switched to safer alternatives, protecting 40 million Americans.

The rail transport of bulk poison gases, such as chlorine gas, anhydrous ammonia, and sulfur dioxide can also pose cyber security risks. Railcars carrying these toxic chemicals could be sabotaged by hackers. Because large quantities (90 tons per car) of these chemicals are frequently transported on over 100,000 miles of unguarded railway, any city they pass through is vulnerable to attacks or accidents.

The railroads themselves realized the danger and were proponents of switching over to safer chemicals. In 2008, the Association of American Railroads issued a statement declaring, “It’s time for the big chemical companies to do their part to help protect America. They should stop manufacturing dangerous chemicals when safer substitutes are available. And if they won’t do it, Congress should do it for them.”

Because real cyber security will most likely not be attained in the foreseeable future, it is imperative that in the case of dangerous chemical facilities, where ever safer alternatives are available they should be required. The EPA’s current proposal preserves the status quo of voluntary measures. But there is still time for the EPA to improve their proposal and include common sense requirements that will protect the lives of millions of workers and community residents.

Source: *http://www.greenpeace.org/usa/why-cyber-security-and-chemical-security-go-hand-in-hand/*